

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-078555

(43)Date of publication of application : 14.03.2000

(51)Int.Cl. H04N 7/16  
H04H 1/02  
H04L 12/14

(21)Application number : 10-243906

(71)Applicant : SONY CORP

(22)Date of filing : 28.08.1998

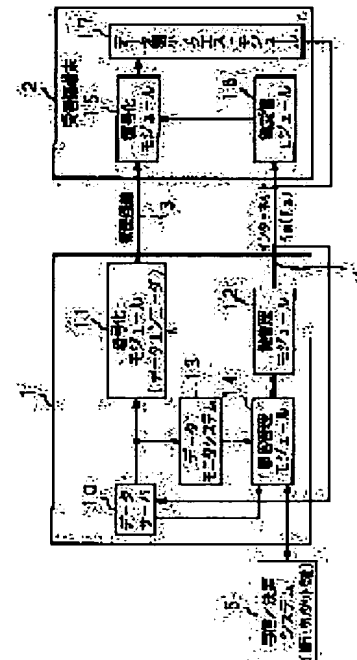
(72)Inventor : KUBOTA ICHIRO

## (54) CHARGING METHOD AND DEVICE FOR DATA TRANSMISSION SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To realize charging for a data unit or a data class and for each contractor while keeping confidentiality of the data in the case of using a high speed data channel with a large capacity such as a digital CATV channel or a satellite broadcast to conduct a data service.

**SOLUTION:** The device has an encryption module that encodes data and serves encrypted data and a key management module 12 that manages an encryption key to decode the encrypted data and the distribution of the encryption key, and the device transmits the encrypted data to a receiver side terminal 2 via a satellite circuit 3 and transmits the encryption key to the receiver side terminal 2 via the Internet 4. A customer management module 14 manages charging of data received by the receiver side terminal 2 depending on a distribution form of the encrypted key transmitted from the key management module 12 to the receiver side terminal 2.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2000-78555

(P2000-78555A)

(43)公開日 平成12年3月14日(2000.3.14)

(51)Int. Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト*(参考)	
H 0 4 N	7/16	H 0 4 N	7/16	C
H 0 4 H	1/02	H 0 4 H	1/02	E
H 0 4 L	12/14	H 0 4 L	11/02	F

審査請求 未請求 請求項の数18 O L

(全18頁)

(21)出願番号 特願平10-243906

(22)出願日 平成10年8月28日(1998.8.28)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 窪田 一郎

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74)代理人 100067736

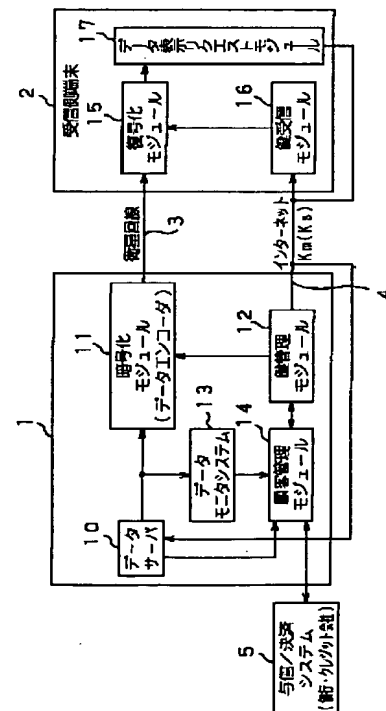
弁理士 小池 晃 (外2名)

(54)【発明の名称】データ伝送システムの課金方法及び装置

(57)【要約】

【課題】 衛星放送やデジタルCATV回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合に、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現する。

【解決手段】 データを暗号化して提供する暗号化モジュール11と、暗号化されたデータの当該暗号化を解くための暗号鍵の管理及びその暗号鍵の配信を管理する鍵管理モジュール12とを有し、暗号化したデータは衛星回線3を介して受信側端末2に送信し、暗号鍵はインターネット4を介して受信側端末に送信する。受信側端末2にて受信したデータに対する課金は、顧客管理モジュール14が、鍵管理モジュール12から受信側端末2に送信された暗号鍵の配信形態に応じて管理する。



## 【特許請求の範囲】

- ・【請求項 1】 通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法において、  
上記データを暗号化して提供し、  
上記暗号化されたデータの当該暗号化を解くための暗号鍵を管理し、  
上記暗号鍵を配信し、  
上記暗号鍵の配信形態に応じて上記課金を管理することを特徴とするデータ伝送システムの課金方法。
- 【請求項 2】 少なくとも通信路が確立される毎に上記暗号鍵を配信することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。
- 【請求項 3】 少なくとも通信路が確立されている時間中に定期的上記暗号鍵を配信することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。
- 【請求項 4】 上記暗号鍵の配信回数を管理し、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 2 記載のデータ伝送システムの課金方法。
- 【請求項 5】 上記暗号鍵の配信回数を管理し、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 3 記載のデータ伝送システムの課金方法。
- 【請求項 6】 通信路が確立されている接続時間を計測し、当該接続時間に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。
- 【請求項 7】 各通信路毎のデータ伝送量を計測し、当該データ伝送量の総和に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。
- 【請求項 8】 伝送するデータ種別により上記暗号鍵を対応させ、当該データ種別による暗号鍵に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。
- 【請求項 9】 上記通信回線は高速の第 1 のデータ伝送路と、当該第 1 のデータ伝送路よりも低速の第 2 のデータ伝送路とからなり、  
上記第 1 のデータ伝送路にて上記暗号化されたデータを伝送し、  
上記第 2 のデータ伝送路にて上記暗号鍵を伝送することを特徴とする請求項 1 記載のデータ伝送システムの課金方法。
- 【請求項 10】 通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金装置において、  
上記データを暗号化して提供するデータ提供手段と、  
上記暗号化されたデータの当該暗号化を解くための暗号

- 鍵の管理及びその暗号鍵の配信を管理する鍵管理手段と、  
上記暗号鍵の配信形態に応じて上記課金を管理する課金管理手段とを有することを特徴とするデータ伝送システムの課金装置。
- 【請求項 11】 上記鍵管理手段は、少なくとも通信路が確立される毎に上記暗号鍵を配信することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。
- 【請求項 12】 上記鍵管理手段は、少なくとも通信路が確立されている時間中に定期的に上記暗号鍵を配信することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。
- 【請求項 13】 上記鍵管理手段は、上記暗号鍵の配信回数を管理し、  
上記課金管理手段は、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 11 記載のデータ伝送システムの課金装置。
- 【請求項 14】 上記鍵管理手段は、上記暗号鍵の配信回数を管理し、  
上記課金管理手段は、当該暗号鍵の配信回数に応じて課金を管理することを特徴とする請求項 12 記載のデータ伝送システムの課金装置。
- 【請求項 15】 通信路が確立されている接続時間を計測する接続時間計測手段を備え、  
上記課金管理手段は、当該接続時間に応じて課金を管理することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。
- 【請求項 16】 各通信路毎のデータ伝送量を計測するデータ伝送量計測手段を備え、  
上記課金管理手段は、当該データ伝送量の総和に応じて課金を管理することを特徴とする請求項 1 記載のデータ伝送システムの課金装置。
- 【請求項 17】 上記鍵管理手段は、伝送するデータ種別により上記暗号鍵を対応させ、  
上記課金管理手段は、当該データ種別による暗号鍵に応じて課金を管理することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。
- 【請求項 18】 上記通信回線は高速の第 1 のデータ伝送路と、当該第 1 のデータ伝送路よりも低速の第 2 のデータ伝送路とからなり、  
上記データ提供手段は、上記暗号化されたデータを上記第 1 のデータ伝送路に伝送し、  
上記鍵管理手段は、上記暗号鍵を上記第 2 のデータ伝送路に伝送することを特徴とする請求項 10 記載のデータ伝送システムの課金装置。
- 【発明の詳細な説明】
- 【0001】
- 【発明の属する技術分野】 本発明は、通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法及び装置に関する。

## 【0002】

・【従来の技術】衛星放送やデジタルケーブルテレビジョン（以下、CATVと記す）回線のような大容量のデータ回線を使用してデータサービスを行う場合には、先行しているデジタルオーディオ／ビデオサービスで用いられているトランスポートストリーム（Transport Stream、以下TSと記す）パケットにインターネットプロトコル（Internet Protocol、以下IPと記す）等のデータパケットを重畳させ、データサービスを行う事が一般的である。

【0003】従って、データサービスの顧客管理を行う上で一番簡単な方法としては、TS毎のスクランブルを行うICカードによる限定アクセス機能（Conditional Access、以下適宜CAと記す）を用いる方法が挙げられる。この場合、TS毎のスクランブルには、TSパケットのパケットID（Packet Identification、以下PIDと記す）によって識別される特定の暗号化キーを用いた、マルチプレクサによるスクランブル処理が行われる。

【0004】例えばインターネットサービスシステムの場合は、送出側において、ある帯域を占有する一つのエンコーダが、サービス（チャンネル）として定義される特定のPIDを持つTSパケットを生成し、このTSパケットの中に、複数ユーザのパーソナルコンピュータ（PC）へのIPデータグラムが多重される。

【0005】ICカードによるCA機器を用いた場合、ユーザグループ（例えば一つの企業）と他のユーザグループの間では、それぞれエンコーダが異なり、違ったスクランブル鍵を持つため、当該スクランブル鍵が破られない限り、互いに相手のデータを盗み見る事は不可能である。

【0006】一方、グループ内では、既にスクランブルが解かれたデータを受信可能であるため、不正に他人のデータを盗み見る事が可能である。但し、ユーザグループが一企業であり、専用線的な使い方をする場合は、特にデータの不正読み出しについて注意を払う必要が無い。

## 【0007】

【発明が解決しようとする課題】しかしながら、一つのサービス（チャンネル）を利用して不特定多数のユーザに対してデータサービスを提供するような時には、この点が問題となる。すなわち、一般のホームページのような、誰でもアクセス可能なデータについては他人に見られても問題は無いと思われるが、いわゆるSOHO（Small Office HomeOffice）のユーザのように、仕事上秘密性の高いデータのやりとりを行う場合には、データを他人に見られる事は非常に問題となり、したがってデータの秘密性を保つ為の手段が必要となる。

【0008】また、衛星放送やデジタルCATV回線等を使用したデータサービスを行う場合、ユーザに提供

したデータに対する課金のシステムを構築しなければならない。衛星デジタル放送では、ICカードによる課金システムが既に構築されているが、このICカードによる課金システムは、元々オーディオ及びビデオ放送の番組単位の課金を基本としたシステムであり、データ単位やデータ種別毎の課金には必ずしも適していない。

【0009】そこで、本発明はこのような状況に鑑みてなされたものであり、衛星放送やデジタルCATV回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合において、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現する、データ伝送システムの課金方法及び装置を提供することを目的とする。

## 【0010】

【課題を解決するための手段】本発明のデータ伝送システムの課金方法及び装置は、通信回線を利用してデータを提供し、このデータ提供に対応した課金を行うデータ伝送システムの課金方法であり、データを暗号化して提供し、その暗号化されたデータの当該暗号化を解くための暗号鍵を管理してその暗号鍵を配信すると共に、そのときの暗号鍵の配信形態に応じて課金を管理することにより、上述した課題を解決する。

## 【0011】

【発明の実施の形態】本発明の好ましい実施の形態について、図面を参照しながら説明する。

【0012】以下、本発明にかかるデータ伝送システムの課金方法及び装置が適用される一実施の形態であるデータサービスシステムの全体構成について、図1を用いて説明する。

【0013】図1に示すデータサービスシステムにおいて、データ送信装置1のデータサーバ10は、例えばオーディオデータやビデオデータ等だけでなく、コンピュータプログラム等の各種データをデジタルコンテンツとして格納してなるものである。本実施の形態では、特にデータサービスを例に挙げているため、当該データサーバ10から取り出されるデジタルコンテンツをコンピュータプログラム等の各種データ（以下、単にデータとする）として説明する。このデータサーバ10から出力されたデータは、暗号化モジュール11に送られる。

【0014】暗号化モジュール（データエンコーダ）11は、鍵管理モジュール12から送られてきた暗号鍵を用いて、上記データサーバ10からのデータを暗号化し、当該暗号化データを、例えば衛星回線やデジタルCATV回線等の大容量且つ高速の通信回線に送信（配信）する。

【0015】ここで、本実施の形態では、通信回線として衛星デジタル放送に使用される衛星回線3を用いた場合を例に挙げている。したがって当該暗号化モジュール11では、上記データサーバ10からのデータをIP（Internet Protocol）等のデータパケットにパケット

化（すなわちIPデータグラムを生成）して暗号化し、この暗号化データ（以下、セクションデータとする）に所定の付加情報（例えばMAC（Media Access Control）アドレスを含むヘッダ等）を付加したデータを、デジタルオーディオ／ビデオサービスで用いられているようなTS（Transport Stream）パケットに重畳させ、当該TSパケットを衛星回線3に送信（すなわち配信）するようにしている。なお、このデータサーバ10におけるIPデータグラムの生成及び暗号化モジュール11における暗号化処理（セクションデータの生成処理）の詳細及び具体的構成、当該セクションデータ及びそのヘッダに含まれるMACアドレス等の詳細については後述する。

【0016】鍵管理モジュール12は、上記暗号化モジュール11におけるIPデータグラムの暗号化に使用する暗号鍵を管理する。この鍵管理モジュール12からの暗号鍵は、電話回線やISDN（Integrated Services Digital Network：統合サービスデジタル通信網）等を使用した地上回線を介して伝送される。本実施の形態では、当該地上回線として、電話回線やISDN等を使用したインターネット4を例に挙げている。上記鍵管理モジュール12がインターネット4を介して受信側端末17に送信する暗号鍵は、セキュリティ確保のため当然暗号化されているものとする。当該鍵管理モジュール12が管理する暗号鍵、及びこの暗号鍵の送信並びに暗号化等の詳細については後述する。

【0017】受信側端末17の鍵受信モジュール16は、上記インターネット4を介して送信されてきた上記暗号鍵を受信して復号（暗号解読）し、当該受信及び復号した暗号鍵を受信側端末17内の復号化モジュール15に転送する。

【0018】復号化モジュール15は、上記衛星回線3を介して受信したデータのTSパケットから前記セクションデータを取り出し、当該セクションデータのヘッダに含まれるMAC（Media Access Control）アドレスに基づいて、対応する暗号鍵を鍵受信モジュール16から受け取り、当該暗号鍵を用いて上記セクションデータ内の暗号化されたIPデータグラムの暗号解読（データデコード）を行う。なお、当該復号化モジュール15における暗号解読の詳細については後述する。

【0019】データ表示リクエストモジュール17は、提供を受けたいデータのリクエストを、例えばインターネット4を通じてデータ送信装置1に送信し、また、必要に応じて表示を行う。

【0020】データ送信装置1のデータモニタシステム13は、個々の契約者の受信側端末2に対して送信（配信）されるデータ量（情報量）や通信路が確立された接続時間などをモニタする。例えば送信されるデータ量をモニタする場合には、送信されるデータのアドレス毎のデータ量或いはパケット毎のデータ量を集計し、また、

接続時間をモニタする場合には、図示しない内部時計からの時間情報に基づいて当該接続時間を集計する。

【0021】また、データ送信装置1の顧客管理モジュール14は、上記鍵管理モジュール12に対して指令を行い、当該鍵管理モジュール12による暗号鍵の配信をどのように行うかを管理する。また、顧客管理モジュール14は、契約者毎の契約形態やデータ単位毎或いはデータ種別毎の課金形態によって様々な課金方法の管理を行うと共に、それら契約形態や課金方法に基づいて契約者毎の課金情報の集計及び管理を行う。さらに、顧客管理モジュール14は、金融／クレジット会社等の与信／決済システム5と回線が繋がっており、したがって、当該顧客管理モジュール14は、当該与信／決済システム17を通して、上記集計された課金情報に基づいた個々の契約者への請求書の発行及び入金管理等を行う。

【0022】ここで、本実施の形態のようなデータサービスシステムにおける契約者の契約形態としては、以下の3種類の契約形態（第1～第3の契約形態）が考えられる。

【0023】「第1の契約形態」データサービスを受ける事が可能な契約を一旦行えば、受信するデータ種別／データ量にかかわらず、一定の課金となされる契約形態（フラット／定額制課金）。

【0024】「第2の契約形態」受信するデータ量によって課金される契約形態（従量制課金）。

【0025】「第3の契約形態」受信するデータ種別によって課金される契約形態（コンテンツ課金）。

【0026】このため、上記顧客管理モジュール14は、データサービスにおいて契約者によりなされる課金設定により、上記第1～第3までの契約形態のうち何れか一つを選択する。

【0027】先ず、上記第1の契約形態（フラット／定額制課金）にて契約がなされた場合、契約者（受信側端末2）は、暗号鍵を一旦受け取った後はそのまま当該暗号鍵を更新する事無く、ずっと使える事になり、最も簡単且つ便利である。

【0028】この第1の契約形態にて契約がなされた場合の課金は、例えば毎月一定額の課金等が考えられ、したがって、上記顧客管理モジュール14では、当該第1の契約形態を選択した契約者に対しては当該毎月一定額となるような課金を、上記与信／決済システム17を通して行う。なお、当該第1の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【0029】ただし、暗号鍵を変更せずに常に同一の暗号鍵を使用していると、例えばハッカー等によって暗号鍵が解明される恐れがある為、一般にはあるタイミングで暗号鍵を変更する必要がある。

【0030】上記暗号鍵を変更するタイミングとしては、以下の3種類の変更タイミング（第1～第3の暗号

鍵変更タイミング)が考えられる。

- ・【0031】「第1の暗号鍵変更タイミング」暗号鍵の不正解読等の問題が発生するまで暗号鍵の変更を行わない。言い換えれば、問題が発生したタイミングで暗号鍵を変更する。

【0032】「第2の暗号鍵変更タイミング」通信路(セッション)が確立される毎に暗号鍵を配信する。すなわち、通信路が確立される毎のタイミングで異なる暗号鍵を配信する。

【0033】「第3の暗号鍵変更タイミング」通信路(セッション)が確立されて通信を行っている時間中は定期的に暗号鍵の配信を行う。すなわち、通信路が確立されて通信を行っている時間中の定期的なタイミングで異なる暗号鍵を配信する。

【0034】これら3つの暗号鍵変更タイミングは第1の暗号鍵変更タイミングから順にセキュリティ性が高くなっており、システムへのセキュリティへの要求度によってどの変更タイミングを取るかを決定すれば良い。

【0035】次に、上記第2の契約形態(従量制課金)にて契約がなされた場合、すなわち、受信するデータ量によって課金を行う場合は、契約者(受信側端末2)が受信したデータ量(言い換えればデータ送信装置1が送信したデータ量)を計測しなければならない。このデータ量の計測方法としては、以下の3種類の計測方法(第1～第3のデータ量計測方法)が考えられる。

【0036】「第1のデータ量計測方法」通信路(セッション)が確立されて通信を行っている時間中は定期的に暗号鍵の配信を行う上記第3の暗号鍵変更タイミングの場合において、通信路(セッション)が確立されている期間中に配信される暗号鍵の配信回数を数え、この配信回数からデータ量を計測する。

【0037】「第2のデータ量計測方法」通信路(セッション)が確立されている期間の接続時間を計り、この接続時間からデータ量を計測する。

【0038】「第3のデータ量計測方法」各通信路(セッション)毎の実際のデータ伝送量を計測する。例えば送信されるアドレス毎或いはパケット数からデータ量を計測する。

【0039】したがって、この第2の契約形態(従量制課金)にて契約がなされた場合の課金は、上記第1～第3のデータ量計測方法の何れを選択したかにより異なる。すなわち、第2の契約形態(従量制課金)にて契約がなされた場合の課金方法としては、上記第1～第3のデータ量計測方法に対応した以下の3種類の課金方法(第1～第3の課金方法)が考えられる。なお、当該第2の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【0040】「第1の課金方法」上記第1のデータ量計測方法のように、通信路(セッション)の確立された期間中に配信された暗号鍵の配信回数からデータ量を計測

した場合は、当該暗号鍵の配信回数に応じて契約者への課金を行う。すなわち、この第1の課金方法の場合の上記顧客管理モジュール14では、通信路(セッション)の確立された期間中に鍵管理モジュール12が受信側端末2に配信した暗号鍵の配信回数を管理し、この配信回数に応じた課金を、上記与信/決済システム17を通して行う。

【0041】「第2の課金方法」上記第2のデータ量計測方法のように、通信路(セッション)の確立された期間中の接続時間を計ってデータ量を計測した場合は、当該接続時間に応じて契約者への課金を行う。すなわち、この第2の課金方法の場合の上記顧客管理モジュール14では、通信路(セッション)の確立された期間中にデータモニタシステム13が集計した接続時間を管理し、この接続時間に応じた課金を、上記与信/決済システム17を通して行う。

【0042】「第3の計測課金方法」上記第3のデータ量計測方法のように、各通信路(セッション)毎のデータ伝送量を直接計測した場合は、当該データ伝送量の総和に応じて契約者への課金を行う。すなわち、この第3の課金方法の場合の上記顧客管理モジュール14では、通信路(セッション)の確立された期間中にデータモニタシステム13が集計したデータ伝送量を管理し、このデータ伝送量の総和に応じた課金を、上記与信/決済システム17を通して行う。

【0043】次に、上記第3の契約形態(コンテンツ課金)にて契約がなされた場合は、受信するデータ種別(コンテンツ)によって課金を行う。すなわち、契約者(受信側端末2)に送信されるコンテンツはそれぞれコンテンツ毎に異なった暗号鍵により暗号化されているため、そのコンテンツを暗号化したときの暗号鍵は予めリクエストの有った契約者(受信側端末2)にのみ配信され、当該暗号鍵を受け取った契約者(受信側端末2)だけが上記暗号化されたコンテンツを正しく復号し、データを取り出すことができるようになっている。このため、当該第3の契約形態のように、受信するデータ種別(コンテンツ)によって課金を行う場合は、契約者(受信側端末2)に受信した暗号鍵(暗号化されたコンテンツの暗号解読を行うための暗号鍵)に応じた課金、言い換えれば契約者(受信側端末2)に対して送信した暗号鍵に応じた課金を行う。なお、この第3の契約形態の場合、課金される金額は、データ種別すなわちコンテンツに応じて異なる額としたり、データの重要度に応じて異なる額とすることも可能である。言い換えれば、契約者(受信側端末2)に送った暗号鍵の種類によって、課金の額を変更することができる。

【0044】したがって、この第3の契約形態の場合の上記顧客管理モジュール14では、鍵管理モジュール12が契約者(受信側端末2)に対して送信した暗号鍵に応じた課金を、上記与信/決済システム17を通して行

う。なお、当該第3の契約形態にて契約がなされた場合における課金のための具体的構成及び動作の詳細については後述する。

【0045】次に、上述したような第1～第2の契約形態にて契約がなされた場合において、課金のための図1の顧客管理モジュール14の具体的構成及び動作について、図2を参照しながら説明する。

【0046】この図2において、顧客管理モジュール14は、個々の契約者毎の契約形態（前記第1～第3の契約形態）及び前記第1～第3の暗号鍵変更タイミング、第1～第3のデータ量計測方法、第1～第3の課金方法についての各情報を顧客情報として格納する顧客データベース21を有すると共に、個々のデータ種別毎のコンテンツリストを格納して個々のデータ種別毎にその情報を管理するコンテンツ管理サーバ20を有している。

【0047】先ず最初に、前記第1の契約形態（フラット／定額制課金）の場合の顧客管理モジュール14における課金処理の流れについて説明する。

【0048】契約者（受信側端末2）から通信路（セッション）確立の要求（リクエスト）がインターネット4等の地上回線を経由してなされた場合、このリクエストは一旦、鍵管理モジュール12に転送される。当該リクエストを受け取った鍵管理モジュール12は、顧客管理モジュール14の顧客認証／鍵管理モジュール制御部23に対して、暗号鍵の配信要求を行う。

【0049】顧客認証／鍵管理モジュール制御部23は、顧客データベース21に格納した顧客情報を用いて、このリクエストを行った契約者の契約情報をチェックし、暗号鍵を与えて良いか否かを判断し、与えて良いと判断された場合は、その顧客情報に記述された鍵配信の形態と合わせて、暗号鍵の配信を鍵管理モジュール12に指示する。また同時に、顧客認証／鍵管理モジュール制御部23は、利用履歴ログ収集部24に対して当該リクエストを行った契約者（受信側端末2）の利用履歴を登録し、利用料課金処理部25に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、さらに請求・収納・支払・滞納管理部26を介して銀行やクレジット会社等の与信／決済システム5に対して契約者への請求書の発行依頼等を行う。

【0050】次に、前記第2の契約形態（従量制課金）を行う場合の顧客管理モジュール14における課金処理の流れについて説明する。

【0051】当該第2の契約形態のように、伝送された情報量（前記暗号鍵の配信回数や接続時間、データ伝送量）に応じた課金を行う場合には、前述したように図1の鍵管理モジュール12における暗号鍵の配信回数や、図1のデータモニタシステム13におけるアドレス毎のデータ量（或いはパケット数）又は接続時間、データ伝送量等の集計情報の取得／集計結果が、顧客認証／鍵管理モジュール制御部23に転送される。顧客認証／鍵管理

理モジュール制御部23では、この集計情報の取得／集計結果に基づいて、利用履歴ログ収集部24に対して当該データの提供を受けた契約者（受信側端末2）の利用履歴のログを取り、利用料課金処理部25に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、請求・収納・支払・滞納管理部26を介して与信／決済システム5に対して契約者への請求書の発行依頼等を行う。

【0052】次に、前記第3の契約形態（コンテンツ課金）を行う場合の顧客管理モジュール14における課金処理の流れについて説明する。

【0053】当該第3の契約形態のように、受信するデータ種別によって課金がなされる場合は、先ずデータサーバ10からコンテンツ課金を行うデータ種別の一覧（コンテンツの一覧）がコンテンツ課金設定部22経由でコンテンツ管理サーバ20に転送されコンテンツリストに載せられることにより、データ種別の登録が行われる。

【0054】コンテンツ課金設定部22では、データ種別すなわちコンテンツ種別とそのコンテンツの暗号化のための暗号鍵の設定を、鍵設定通知として鍵管理モジュール12に指示する。

【0055】ここで、一旦、コンテンツ管理サーバ20にデータ種別が登録されれば、後は第1の契約形態（フラット課金／定額制課金）の場合と同様の処理が行われる。すなわち、特定のデータ種別（特定のコンテンツ）の配信の要求（リクエスト）があった場合、顧客認証／鍵管理モジュール制御部23は、当該要求者が顧客データベース21に登録された契約者であるか否かを判断し、またこのリクエストを行った契約者の契約情報をチェックし、暗号鍵を与えて良いか否かを判断し、さらに、与えて良いと判断された場合に、そのリクエストされたデータ種別がコンテンツ管理サーバ20のコンテンツリストに登録されているかの確認を行い、当該リクエストのあったデータ種別がコンテンツリストに登録されていると確認した場合には、そのリクエストされたデータ種別に対応する鍵配信を鍵管理モジュール12に指示する。また同時に、顧客認証／鍵管理モジュール制御部23では、利用履歴ログ収集部24に対して配信の要求を行った契約者とそのリクエストされたデータ種別の利用履歴の登録を行い、利用料課金処理部25に対して例えば毎月のある期日にその利用状況に応じた課金処理を行い、請求・収納・支払・滞納管理部26を介して与信／決済システム5に対して契約者への請求書の発行依頼等を行う。

【0056】次に、本発明実施の形態のデータサービスシステムのより概略的な構成、前記データサーバ10でのIPデータグラム生成及び暗号化モジュール11における暗号化処理（セクションデータの生成処理）の詳細及び具体的構成、当該セクションデータ及びそのヘッ

10

20

30

40

50

ダに含まれるMACアドレス等の詳細、鍵管理モジュール12が管理する暗号鍵及びこの暗号鍵の送信並びに暗号化等の詳細、復号化モジュール15における暗号解読の詳細について、以下に説明する。

【0057】本発明実施の形態のデータサービスシステムは、図3に示すように、通信経路とされる衛星回線3、専用線37、電話回線38、及び双方向の通信経路39を介して、前記データ送信装置1から前記受信側端末2であるデータ受信装置2a、2b、2cに対してデータを配信するようになされており、上記データ送信装置1でデータを暗号化し、当該暗号化したデータをデータ受信装置2a、2b、2cに通信経路を介して伝送するデータサービスシステムである。

【0058】このデータサービスシステムは、データ送信装置1からデータ受信装置2a、2b、2cへのデータの伝送に使用する第1の通信経路とされる通信衛星34を利用した通信経路と、データ送信装置1とデータ受信装置2a、2b、2cとの間を双方向通信可能にする第2の通信経路である専用線37、電話回線38、及び双方向の通信経路39とを有している。そして、データサービスシステムは、データ送信装置1からデータ受信装置2a、2b、2cへ送る暗号化したデータの伝送には、上記第1の通信経路を用い、データ送信装置1からデータ受信装置2a、2b、2cへの前記暗号鍵の伝送には、上記第2の通信経路を用いている。第2の通信経路は、前記インターネット4と接続されている。

【0059】上記データ送信装置1は、上記各通信回線を利用してデータ受信装置2a、2b、2cへの各種データの配信を行う。データ受信装置2a、2b、2cは、各通信回線から伝送されてくるデータを受信する。なお、図1には、データ受信装置2a、2b、2cを3台として示しているが、実際には数百台から数万台のデータ受信装置（受信側端末2）が存在して当該データサービスシステムを構成している。

【0060】このデータ送信装置1とデータ受信装置2a、2b、2c（なお、以下の説明では、データ受信装置2a、2b、2cについて特定する必要がない場合には、単にデータ受信装置2という。）との間でデータの送受信を可能にする通信経路については、次のように構成されている。

【0061】上記衛星回線3は、約30Mbpsの帯域を持ったKuバンドの片方向の回線を想定する。この衛星回線3により、例えば、日本全国に分布されているデータ受信装置に対して、データ送信装置1からのデータの伝送を同時期に行うことができる。

【0062】双方向の通信経路39は、データ送信装置1とデータ受信装置2との間で、衛星回線3とは別に設けた通信経路であって、データ送信装置1とデータ受信装置2との間で双方向通信を可能にするものである。本実施の形態では、双方向の通信経路39は、イン

ターネット4での通信に用いる汎用の通信経路を想定している。

【0063】専用線37は、データ送信装置1とデータ受信装置2とを直接接続している通信手段である。

【0064】上記インターネット4は、いわゆる映像情報、音楽情報等の各種情報を提供するものであって、いわゆるインターネットサービスプロバイダ35により、インターネット4とデータ受信装置2とは通信可能に接続されている。データ送信装置1は、インターネット4に接続されている。

【0065】なお、上述したようにデータ送信装置1とデータ受信装置2との間でデータの送受信を可能にする専用線37、電話回線38、及び双方向の通信経路39は、衛星回線3ほど大容量の帯域ではなく、数Kbpsから数百Kbps程度が通常の帯域とされる。

【0066】上記データサービスシステムは、所定のデータを特定のデータ受信装置においてのみ受信することが可能になされており、例えばデータ受信装置2aのみにデータを伝送するといった個別配信（ユニキャスト型データ配信）、又は例えばデータ受信装置2a、2bとからなる受信グループにのみデータを伝送するといったグループ宛の同報配信（マルチキャスト型データ配信）、又は全てのデータ受信装置2a、2b、2cに同時にデータを伝送するといった一斉配信（ブロードキャスト型配信）等の配信形態が可能とされて構成されている。

【0067】次に、このデータサービスシステムにおいて、データ送信装置1からデータ受信装置2へのデータの伝送について説明する。

【0068】データ送信装置1からデータ受信装置2へ伝送されるデータは、図4に示すように、データのカプセル化が施されている。このカプセル化は、データを伝送するデータ送信装置1において行われる処理であって、第1のカプセル化工程により、データ受信装置2への配信対象とされるデータを第1のプロトコルによりカプセル化し、第2のカプセル化工程により、上記第1のプロトコルによりカプセル化したデータを第2のプロトコルによってカプセル化する。ここで、カプセル化とは、データ自体に対して加工を施すことなく、当該データ自身を通信プロトコルにより規定された伝送フォーマットに基づいて構成されるカプセル（パケット又はフレーム等）に入れ込むことをいい、このカプセル化によりデータの伝送制御が可能になる。

【0069】上記第1のカプセル化工程では、データ受信装置2への配信対象とするデータの全体を含む実データ部に当該実データ部に関する付加情報部を付加してカプセル化するとともに、上記実データ部については暗号化して上記カプセル化を行う。以下に詳しく説明する。

【0070】IP（Internet Protocol）データグラム101は、図4の（a）に示すように、インターネット

10

20

30

40

50



プロトコルに則して構成されているデータである。このIPデータグラム101は、上記データ受信装置2への配信対象とされるデータを格納して構成されている。そして、IPデータグラムのヘッダ部には、例えば、インターネット上において使用される宛先を識別するための送信先アドレス (Destination Address) が付加されている。

【0071】なお、IPデータグラム101の部分は、インターネットプロトコルとして構成されることに限定されるものではなく、イーサネットプロトコルを採用して構成されてもよい。

【0072】そして、データ送信装置1は、図4の(b)から図4の(d)に示すように、データを上記第1のプロトコルによりカプセル化する。例えば、第1のプロトコルとしては、DVB (Digital Video Broadcasting) のMultiprotocol Encapsulationを採用している。

【0073】まず、データ送信装置1は、第1のプロトコルによるデータのカプセル化を、図4の(b)に示すように、IPデータグラムに対してパディングを行い (パディング部102を付加する)、データ部の長さを64ビットの整数倍にする。例えば、IPデータグラム101の末尾に0ビット〜63ビット長のパディングを行い、パディングするビットはすべて1とする。このパディングにより、所定のデータ長にすることができ、これは、このIPデータグラム101とパディング部102とからなるセクションのデータ部を暗号化する際に、データ部の長さが64ビットの整数倍の方が都合が良いからである。本実施の形態では、当該第1のプロトコルのフォーマットによって構成されるデータ部分をセクションと呼んでいる。

【0074】次に、データ送信装置1は、パディング部102が付加されたセクションを、図4の(c)に示すように暗号化する。ここで、暗号化は、暗号鍵によって行うもので、暗号鍵は、上記データ受信装置2に対して配信の対象とされる情報について暗号化するために使用される後述するセッション鍵である。また、暗号化の方式としては、いわゆるTriple-DESのような共通鍵方式のブロック暗号化を用いる。このTriple-DES方式の暗号化は、公開鍵方式の中でも強力な暗号方式であり、ハードウェアによる実装で高速化も容易とされる。これにより、30Mbps程度の高速な暗号化にあっても、公開鍵方式の暗号化とは異なり、処理時間がかかってデータの伝送が間に合わなくなることを防止することができる。

【0075】そして、データ送信装置1は、図4の(d)に示すように、暗号化されたセクションデータ部104に、セクションヘッダ部103及びエラー検出のために使用されるテイラ部105を付加する。

【0076】ここで、上記暗号化されたセクションデー

タ部104は、MAC (Media Access Control) フレーム化されて構成されている。このMACフレーム化により、データ部にMACヘッダが付加され、このMACヘッダ部を参照することにより、当該フレーム化されて格納されているデータの宛先の制御が容易となされるようになる。具体的には、MACフレームには、当該MACフレーム化されたデータの受信が許可されているデータ受信装置の宛先アドレスが格納されている。

【0077】上記セクションヘッダ部103は、宛先アドレスを格納する部分であって、48ビットの宛先アドレスが格納されるようにデータ空間が確保されている。具体的には、上記セクションヘッダ部103においてMACヘッダ部を構成して、宛先アドレスが格納されている。このセクションヘッダ部103に48ビットにより表現される宛先アドレスを格納できる空間を設けることにより、データ受信装置の限定範囲の種類が少ないことを解消することができる。すなわち、暗号鍵を識別するための多くの情報を格納することができるようになる。さらに、IPデータグラム101を伝送する際に、インターネットプロトコルの宛先アドレスから後述するパケットIDの対応付けを行わなくもよくなり、インターネットプロトコルとの親和性を得ることができる。

【0078】また、上記テイラ部105は、CRC (Cyclic Redundancy Checking、巡回冗長検査) によってコード化されている。CRCは、MACフレーム化されたデータを受信したデータ受信装置2が、当該MACフレームが正しく衛星回線において伝送されているかを検査するためのものである。例えば、CRCは、32ビットによってコード化されている。

【0079】以上が第1のプロトコルによる配信対象とされるデータのカプセル化であって、次に、この第1のプロトコルによってカプセル化されたデータを、第2のプロトコルによってカプセル化させる処理について説明する。

【0080】第2のプロトコルによるカプセル化は、上記第1のプロトコルによってカプセル化されたデータを、複数のパケットに分割することにより実行されるカプセル化である。

【0081】ここで、第2のプロトコルは、TS (Transport Stream) パケット化によるものである。MPEG 2 (Moving Picture Experts Group Phase 2) によって規格されているものであって、オーディオ、ビデオ信号やデータのような多種類のデータが多重化されて、大容量のデジタル回線で伝送することが可能になる。この第2のプロトコルにより、上記第1のプロトコルによってカプセル化されたデータは、図4の(e)乃至図4の(g)に示すように、カプセル化されて、複数のTSパケット106、107、108に分割される。上記TSパケット106、107、108は、TSヘッダ部HTSと、TSペーロード部Pとによって構成され、上記TS

ペイロード部Pには、分割されて上記第1のプロトコルによってカプセル化されたデータが格納される。そして、TSパケットのTSヘッダ部HTSには、図5に示すような、パケットID(PID)部及びスクランブル制御部によって構成される。この図5は、一般的なTSパケットのフォーマットの構造を表しており、ヘッダ部のPID(Packet Identification)部411及びスクランブル制御部412により暗号鍵が特定される。当該暗号鍵は、セッション鍵Ksとワーク鍵Kmとがある。また、上記PID部411は13ビットのデータであり、上記スクランブル制御部412は2ビットのデータ、TSパケットのデータはペイロード部分413に記述される。なお、この図5の例では、PID部411及びスクランブル制御部412に宛先アドレスが書き込まれているが、本実施の形態においては、上述したように、宛先アドレスをセクションヘッダ部103に書き込むことにより、宛先アドレス情報が制限されることを防止している。

【0082】以上が第2のプロトコルによるカプセル化であり、よって、データ送信装置1は、データ受信装置2への配信対象とされるデータ(IPデータグラム)を第1のプロトコル及び第2のプロトコルによって多重にカプセル化して、通信衛星34への当該データの伝送を行っている。

【0083】このように、本実施の形態では、TSパケットとセクションの2つのレベルにおいてそれぞれ独立に処理してデータ伝送を行っているので、例えば利用するPIDを増加することなく、暗号鍵について多くの情報を確保することができ、また、アプリケーション毎に制御方法を用意しなくて済み、新しいアプリケーションへの素早い対応がでいるようになり、さらに、認証ヘッダや暗号ペイロードを既存のインターネットで使うことができるようになる。

【0084】次に、データ送信装置1において行う暗号鍵によるデータの暗号化及びデータ受信装置2において行う暗号化されているデータの暗号鍵(復号鍵)による復号化について説明する。

【0085】ここで、データ送信装置1における前記鍵管理モジュール12及び暗号化モジュール11と、データ受信装置2の前記鍵受信モジュール16及び復号化モジュール15は、具体的には図6に示すように構成されている。

【0086】この図6において、セッション鍵Ks124及び134は、上記データ送信装置1及び上記データ受信装置2がデータの暗号化/復号化に使用する鍵であり、いわゆる共通鍵方式が採用されている。上記データ送信装置1のセッション鍵Ks124は前記鍵管理モジュール12が管理し、上記データ受信装置2のセッション鍵Ks134は鍵受信モジュール16が復号化して生成する。

【0087】データ送信装置1の暗号化ユニット121は、セッション鍵Ks124を使用して、特定のデータ受信装置に対して送られる情報データを暗号化する。すなわち図1の暗号化モジュール11は、図4の(c)に示すセクションのデータ部を、当該セッション鍵Ks124を使用して上記Triple-DESにより暗号化する。また、データ受信装置2の復号化ユニット131は、配信されてきた暗号化されたデータをセッション鍵Ks134により復号化して意味のある情報として取り出す。

10 【0088】マスター鍵Km125及びKm135は、上記セッション鍵Ksと同様に、データ送信装置1及びデータ受信装置2が共に所持している暗号鍵であって、各データ受信装置2a、2b、2cに固有のものである。

【0089】マスター鍵Kmは、データ送信装置1とデータ受信装置2と間を送信処理されるようなことはなく、すなわち、通信経路上に存在する場合はなく、これによりいかなる手段によっても他人によって知ることができない暗号鍵とされている。

20 【0090】このマスター鍵Kmは、セッション鍵Ksをデータ送信装置1からデータ受信装置2に送信する際に、セッション鍵Ksを暗号化/復号化するために用いられる。すなわち、データ送信装置1の鍵管理モジュール12に内蔵される暗号化ユニット122は、マスター鍵Km125を使用してセッション鍵Ks124を暗号化してデータ受信装置2に予め伝送しておく。データ受信装置2の鍵受信モジュール16に内蔵される復号化ユニット132は、受信した暗号化されているセッション鍵Ks124を、当該データ受信装置2が所持しているマスター鍵Km135によって復号化して取り出す(セッション鍵Ks134として取り出す)。

30 【0091】このマスター鍵Kmによる暗号鍵(セッション鍵Ks)の暗号化及び復号化により、データ送信装置1からデータ受信装置2へ伝送する間に、上記暗号化されたセッション鍵Ksが盗聴者によって盗聴されたとしても、その復号化がなされることはない。

【0092】なお、このマスター鍵Kmによるセッション鍵Ksの暗号化/復号化についても、上記Triple-DESに基づいて行うが、公開暗号方式を採用することもできる。これは、公開暗号方式は、鍵の暗号化及び復号化がデータの暗号化/復号化とは異なり高速性を要求されないこと、安全性を確保することができるからである。

【0093】本実施の形態では、上記セッション鍵Ks124を、前述したように顧客管理モジュール14の管理の元で鍵管理モジュール12が管理し、このセッション鍵Ks124の配信状況に応じて前述したような課金が行われる。

50 【0094】ここまでの説明では、データ受信装置2がデータ送信装置1から受動的にセッション鍵Ks124を受け取る例を説明したが、双方向通信経路9を利用す

ることにより、データ受信装置 2 の側から能動的にセッション鍵 K s の要求を行うこともできる。これにより、各データ受信装置 2 a, 2 b, 2 c は、素早く確実に必要なセッション鍵 K s 1 2 4 をデータ送信装置 1 から取得することができる。具体的には、例えば、新たにデータ受信装置 2 がこのデータサービスシステムに加わる場合や、障害によりこの系から外れていたデータ受信装置 2 が障害から復旧して再びこのデータサービスシステムに加わる場合、またデータ受信装置 2 においてセッション鍵 K s が正しく受信出来なかった場合などには、データ受信装置 2 の側から能動的にセッション鍵 K s の要求を行うことにより、各データ受信装置 2 a, 2 b, 2 c は素早く確実に必要なセッション鍵 K s を取得することができる。例えば、上述したような障害復旧やセッション鍵 K s の更新の管理は、データ送信装置 1 の鍵管理モジュール 1 2 や、データ受信装置 (受信側端末) 2 内にある鍵受信モジュール 1 6 及びデータ表示リクエストモジュール 1 7 等が、双方向に通信を行うことにより実現する。このようなことから、本実施の形態においては、例えば衛星回線のみをデータサービスシステムに組み込むことによる弊害、例えば、情報が各データ受信装置に正しく伝わったかどうかをデータ送信装置が知ることができない等といった問題を解決することができる。

【0095】なお、データ送信装置 1 からデータ受信装置 2 へのセッション鍵 K s の伝送については、片方向通信経路とされる衛星回線 3 を用いて行ってもよく、双方向の通信経路 3 9 によって行ってもよい。

【0096】ここで、上記セッション鍵 K s は、前記第 3 の暗号鍵変更タイミングのように、定期的に更新して配信される場合がある。このセッション鍵 K s の更新は、図 7 に示すフローチャートのような更新手順に従って実行される。

【0097】まず、ある時点において、データ受信装置 2 の鍵受信モジュール 1 6 は、セッション鍵 K s 1 3 4 として、セッション鍵 K s\_even と、セッション鍵 K s\_odd の 2 つを保持している。データ受信装置 2 は、このようにセッション鍵 K s を 2 つ所持することにより、このセッション鍵 K s\_even 又はセッション鍵 K s\_odd の何れかを使用して、データ送信装置 1 から送信されてくる情報データの復号化を行う。

【0098】ここで、現在使っているセッション鍵 K s がどちらであるかは、前記図 4 に示すセッションヘッダ部 1 0 3 に情報として書き込まれている。例えば、セッションヘッダ部 1 0 3 は、図 8 に示すように、テーブル I D (table\_id)、MAC アドレス部 (MAC\_address\_1, MAC\_address\_2, MAC\_address\_3, MAC\_address\_4, MAC\_address\_5, MAC\_address\_6) と、セクション情報部 (section\_length, section\_number, last\_section\_number)、s s i (section\_syntax\_indicator)、p i (private\_indicator)、r s v d (reserved)、p s c (payload\_scr

amble\_indicator) 1 1 1、a s c (address\_scramble\_indicator)、L S f (LLC\_SNAP\_flag)、及び c n i (current\_next\_indicator) によって構成されている。ここで、p s c 1 1 1 が現在使っているセッション鍵 K s がどちらであるかの情報を示す。例えば、上記 p s c 1 1 1 は、2 ビットの情報であり、例えば、p s c の上位ビットが「0」のときは、セッション鍵 K s\_even が使用されていることを示し、p s c の上位ビットが「1」のときには、セッション鍵 K s\_odd が使用されていることを示す。

【0099】上述したような使用されているセッション鍵 K s の判断をステップ S 1 において行った後、データ受信装置 2 の鍵受信モジュール 1 6 は、ステップ S 2 において、タイマーでトリガをかけ、セッション鍵 K s の更新タイミングを知る。

【0100】続いて、データ受信装置 2 の鍵受信モジュール 1 6 は、ステップ S 3 において、MAC アドレスとセッション鍵 K s の対応表にある現在のセッション鍵 K s のフラグを更新する。データ受信装置の鍵受信モジュール 1 6 は、例えば、図 9 の MAC アドレスとセッション鍵 K s の対応表を有しており、この対応表を参照して、現在のセッション鍵 K s のフラグ 1 1 2 を更新する。この更新処理により、上記の p s c 1 1 1 の上位 1 ビットが反転する。例えば、p s c の上位ビットが「0」に反転される。

【0101】そして、データ受信装置 2 では、ステップ S 4 において、その p s c に基づいてそのセクションに含まれている I P データグラムの復号化を行う。すなわち、p s c の上位ビットが「0」とされた場合には、データ受信装置 2 の鍵受信モジュール 1 6 は、これまで使用していたセッション鍵 K s\_odd (p s c の上位ビットが「1」のとき使用されるセッション鍵 K s) からセッション鍵 K s\_even に変更し、復号化モジュール 1 5 ではこのセッション鍵 K s\_even により復号化を行う。また、p s c の上位ビットが「1」とされた場合には、データ受信装置 2 の鍵受信モジュール 1 6 は、これまで使用していたセッション鍵 K s\_even (p s c の上位ビットが「0」のとき使用されるセッション鍵 K s) からセッション鍵 K s\_odd に変更し、復号化モジュール 1 5 ではこのセッション鍵 K s\_odd により復号化を行う。

【0102】そして、次のセッション鍵 K s の切替えのタイミングまでの間に、ステップ S 5 において、データ送信装置 1 の鍵管理モジュール 1 2 では、次のセッション鍵 K s をマスター鍵 K m 1 2 4 により暗号化してデータ受信装置 2 に転送する。

【0103】なお、暗号化されたセッション鍵 K m (K s) の転送は、衛星回線 3 又は双方向の通信回線 3 9 を使って伝送するが、その伝送の際のプロトコルについては、応答の伴うプロトコルを用い、例えば T C P / I P (Transmission Control Protocol / Internet Protocol

10

20

30

40

50

1) を使用する。これにより、データ送信装置 1 からデータ受信装置 2 へのセッション鍵 Ks の伝送が確実に行われる。

【0104】そして、この転送処理の間に、ステップ S6 において、データ受信装置 2 の鍵受信モジュール 16 は、図 9 に示す MAC アドレスのセッション鍵 Ks の対照表の更新を行う。すなわち、以前使用していたセッション鍵 Ks を、新しいセッション鍵 Ks に書き換える処理を行う。

【0105】その後、ステップ S7 において、データ受信装置 2 の鍵受信モジュール 16 は、対象とするデータ受信装置 2 に次のセッション鍵 Ks が保持されたかを確認した後に、ステップ S8 に進み、次のセッション鍵 Ks に切り替える。ここで、ステップ S8 以降ステップ S13 までの処理は、psc の上位ビットが「1」とされて、セッション鍵 Ks<sub>odd</sub> を復号化に使用するときの処理であって、上記ステップ S7 から進む処理であり、また、上記ステップ S1 において、データ受信装置 2 にて現在のセッション鍵 Ks がセッション鍵 Ks<sub>even</sub> (psc の上位ビットが「0」) とされたときに実行される処理でもある。

【0106】上述したような手順により、データ送信装置 1 は、更新されるセッション鍵 Ks を確実にデータ受信装置 2 に届けることができ、データ受信装置 2 では、2 つ所持するセッション鍵 Ks を切替えを瞬時にし、データの取りこぼしもなくセッション鍵 Ks による復号化を実現することができる。なお、伝送処理時間の許す範囲で、セッション鍵 Ks 124 の更新頻度は柔軟に変更することが可能である。

【0107】以上のようにセッション鍵 Ks がデータ送信装置 1 において逐次変更されている場合でも、データ受信装置 2 は、このように変更されるセッション鍵 Ks によって暗号化されているデータの復号が可能である。

【0108】次に、データ送信装置 1 がデータを送信するまでの手順、及びデータ受信装置 2 がデータを受信したときの手順について説明する。データ送信装置 1 がデータを送信するまでの手順については、例えば、図 10 に示すフローチャートに従って実行している。そして、データ受信装置 2 がデータを受信してからの手順については、例えば、図 11 に示すフローチャートに従って実行している。

【0109】まず、データ送信装置 1 がデータを送信するまでの手順については、ステップ S21 において、データ送信装置 1 は、データ受信装置 2 に伝送する IP データグラムを、データ送信装置 1 自身又は双方向の通信経路 39 に繋がるインターフェースより、受け取る。また、インターネット 4 上からのアクセス情報に基づいて、情報センタの情報の提供を受け取る。

【0110】次にステップ S22 において、データ送信装置 1 は、IP データグラムの宛先アドレスを見て、第

1 のプロトコルの宛先アドレスを知る。例えば、データ送信装置 1 は、当該データ送信装置 1 内に所持している図 12 に示すような IP アドレスと MAC アドレスの対応表からデータ受信装置 2 の第 1 のプロトコルでの宛先アドレスを知る。

【0111】そして、宛先アドレスを知ったデータ送信装置 1 は、その宛先アドレスをもとに上記セクションを作成する。ここで、データ送信装置 1 は、必要に応じてデータ部にビット 1 によるパディングを行い、データ部が 64 ビットの倍数になるようにする。

【0112】次に、ステップ S23 において、例えば図 9 に示したような MAC アドレスとセッション鍵 Ks の対応表から現在のセッション鍵 Ks のフラグ 112 を見て、現在使用しているセッション鍵 Ks 124 を取り出し、当該取り出したセッション鍵 Ks により、上記図 4 の (c) に示すように、セクションのデータ部を暗号化する。その際、現在のセッション鍵 Ks のフラグを見て、その内容を上記図 9 に示すセッションのヘッダ部の psc 111 の上位 1 ビットに入れる。

【0113】次にステップ S24 において、図 4 の (e) 乃至図 4 の (g) に示すように、このセクション全体 109 を分割して各 TS パケット 106, 107, 108 のペイロード部 P に入れ、当該 TS パケット 106, 107, 108 に予め定められた上記 PID を付加し、さらに、第 2 のプロトコルの必要に応じてペイロード部 P を暗号化し、衛星回線 3 に送出する。

【0114】以上がデータ送信装置 2 がデータを送信するまでの手順である。そして、データ受信装置 2 では、上述のようにして衛星回線 3 に送出されたデータを受信する。

【0115】データ受信装置 2 は、先ず図 11 のステップ S31 において、衛星回線 3 より受信した TS パケット 106, 107, 108 を第 2 のプロトコルに従って復号化し、セクション全体 109 を再構築する。

【0116】次に、ステップ S32 において、データ受信装置 2 は、セクションの宛先アドレス (MAC アドレス) を取り出し、続いて、ステップ S33 において、図 13 に示す MAC アドレスとセッション鍵 Ks の対応表を参照して MAC アドレスが存在するか否かの判別処理を行う。すなわち、自己に送信が許可されているデータを格納しているものであるか否かの判別処理を行う。ここで、MAC アドレスがないことを確認した場合には、データ受信装置 2 は、ステップ S34 に進み、そのデータの破棄の処理を行う。また、MAC アドレスがあることを確認した場合には、データ送信装置 2 は、ステップ S35 に進み、セクションヘッダ部 103 より前記図 8 に示した psc 111 を取り出す。そして、データ送信装置 2 は、その psc 111 の上位 1 ビットから現在有効なセッション鍵 Ks がどちらであるかを調べ、2 つのセッション鍵 Ks から現在有効とされるセッション鍵 K

sを取り出す。

【0117】データ受信装置2は、このようにして取り出したセッション鍵Ksにより、ステップS36において、セクションデータ部104をTriple-DESにより復号化する。

【0118】そして、データ受信装置2は、ステップS37において、当該復号したデータからIPデータグラムを取り出す。例えば、IPデータグラムの取り出しは、復号化されたデータ部の先頭にあるIPヘッダから図14のTOTAL LENGTH フィールド113を読み取り、IPデータグラムの長さを調べ、そこから計算されるIPデータグラム全体を取り出す。これにより、暗号化の際に付加した余計なパディングを除去される。このようにして目的とするIPデータグラムを取り出すことができる。

【0119】以上のような手順により、データ送信装置1は、データを送信するまでの処理を行い、また、データ受信装置2は、受信したデータに対する処理を行い、自己に宛てて配信されてきた情報データを受け取る。

【0120】なお、本実施の形態のデータサービスシステムは、次のように変形することも可能である。

【0121】すなわち、第1の変形例として、データサービスシステムは、図15に示すように構成することも可能である。この図15に示すデータサービスシステムは、データ受信装置2がIPルータとして構成される場合である。

【0122】ところで、上述したデータサービスシステムでは、データ受信装置2が直接IPデータグラムを受信する構成としている。しかし、このデータサービスシステムでは、データ受信装置2をIPルータとして構成することにより、データ受信装置2が衛星回線3から受信したデータを、イーサネットなどのローカルエリアネットワーク(LAN)202を経由してつながっている衛星回線3へのインターフェースを持たないコンピュータ203a, 203bにもデータを伝送することができる。その際、データ送信装置1やデータ受信装置2は、データ受信装置2だけでなく、それがつながっているローカルエリアネットワーク202上のコンピュータ203a, 203b全てについてのデータの配信を行うことができるようになる。具体的には、図12に示したデータ送信装置1内のIPアドレスとセクションの宛先アドレス(MACアドレス)の対応表のIPアドレスが、個別のIPアドレスではなく、複数のIPアドレスの集合を示すIPのネットワークアドレスに変わることになる。但し、このデータサービスシステムにおいて、データ伝送を行うのは衛星回線3の区間のみであるため、データ受信装置2とコンピュータ203a, 203bとの間でもデータ配信を行うには、IPプロトコル又はそれより上位のアプリケーションのレベルでのデータ配信制御が必要となる。

【0123】次に、第2の変形例として、データサービスシステムは、図16に示すように構成することも可能である。このデータサービスシステムでは、データ受信装置2がブリッジとして構成され、IPデータグラムを伝送するプロトコルの変換のみを行い、上記データ伝送システム201とでは、ルーティングを行わないことである。

【0124】この場合の上記データ受信装置2は、衛星回線3より受信したデータを復号化してIPデータグラムを取り出し、それをイーサネットフレームに入れて汎用のルータ302に転送する。そして、汎用のルータ302が、通常のIPデータグラムに対する処理を行う。これにより、ルーティングを行わないためにデータ受信装置2の構成が簡単になり、既存の汎用のルータを用いることができるようになる。

【0125】

【発明の効果】以上の説明で明らかなように、本発明においては、データを暗号化して提供し、暗号化されたデータの当該暗号化を解くための暗号鍵を管理し、暗号鍵を配信し、暗号鍵の配信形態に応じて課金を管理することにより、例えば衛星放送やデジタルCATV回線のような大容量で高速なデータ回線を使用してデータサービスを行う場合において、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現可能としている。

【0126】すなわち本発明のデータ伝送システムの課金方法及び装置は、例えば衛星放送や双方向或いは一方のデジタルCATV回線等の大容量且つ高速のデータ伝送路と、電話回線やISDN等に代表される比較的低速度の回線とを組み合わせることにより、高速のインターネットアクセス等のデータサービスを実現すると共に、IPパケットベースの暗号化における鍵配信の仕組みとデータ提供に対する課金とを組み合わせることにより、データの秘密性を維持しつつデータ単位やデータ種別毎の課金、更には契約者毎の課金を実現可能としている。

【図面の簡単な説明】

【図1】本発明のデータ伝送システムの課金方法及び装置が適用されるデータサービスシステムの主要部の構成を示すブロック図である。

【図2】本実施の形態のデータサービスシステムの顧客管理モジュールの構成例を示すブロック図である。

【図3】本発明の実施の形態であるデータサービスシステムの概略的な構成を示す図である。

【図4】本実施の形態のデータサービスシステムを構成するデータ送信装置からデータ受信装置へ送信されるデータであって、複数のプロトコルによってカプセル化が施されたデータを示す図である。

【図5】TSパケットのデータ構造のフォーマットを示す図である。

【図6】データ送信装置及びデータ受信装置の構成を示すブロック図である。

【図7】データ送信装置からデータ受信装置へ送信されるデータを暗号化するセッション鍵の変更を行う手続きの一連の工程を示すフローチャートである。

【図8】セクションヘッダのデータ構造を示す図である。

【図9】MACアドレスとセッション鍵のフラグとの対応表を示す図である。

【図10】データ送信装置において行うデータのカプセル化の一連の手続きを示すフローチャートである。

【図11】データ受信装置が受信したデータをセッション鍵により復号化するときの一連の手続きを示すフローチャートである。

【図12】IPアドレスとMACアドレスとの対応表を示す図である。

【図13】MACアドレスとセッション鍵の対応表を示す図である。

【図14】IPデータグラムの取り出しの際に使用されるTOTALLENGTHフィールドが格納されるデータ構造を示す図である。

す図である。

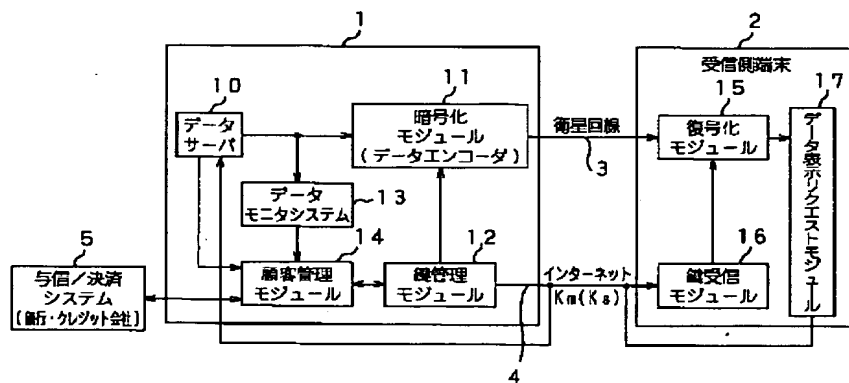
【図15】本実施の形態のデータサービスシステムの第1の変形例を示す図である。

【図16】本実施の形態のデータサービスシステムの第2の変形例を示す図である。

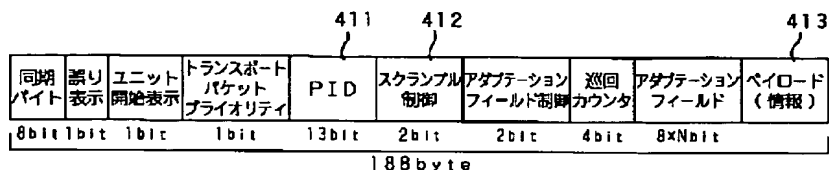
【符号の説明】

1 データ伝送装置、 2 受信側端末（データ受信装置）、 3 衛星回線、 4 インターネット、 5 与信/決済システム、 10 データサーバ、 11 暗号化モジュール（データエンコーダ）、 12 鍵管理モジュール、 13 データモニタモジュール、 14 顧客管理モジュール、 15 復号化モジュール、 16 鍵受信モジュール、 17 データ表示リクエストモジュール、 20 コンテンツ管理サーバ、 21 顧客データベース、 22 コンテンツ課金設定部、 23 顧客認証/鍵管理モジュール制御部、 24 利用履歴ログ収集部、 25 利用料課金処理部、 26 請求・収納・支払・滞納管理部、 Ks セッション鍵、 Km マスター鍵

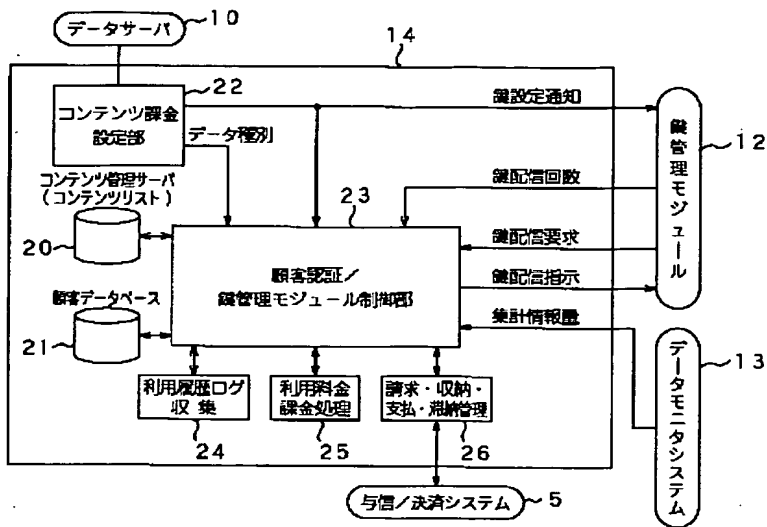
【図1】



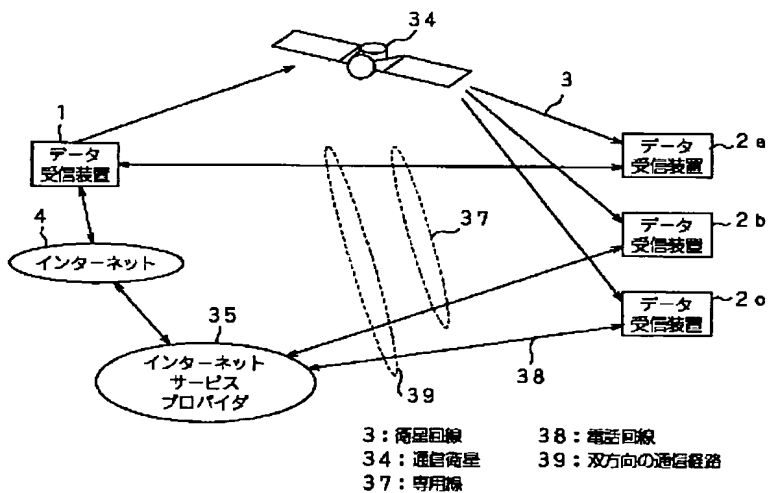
【図5】



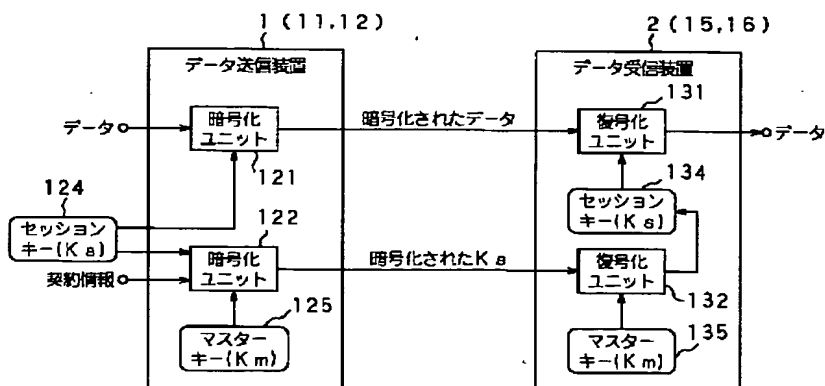
【図2】



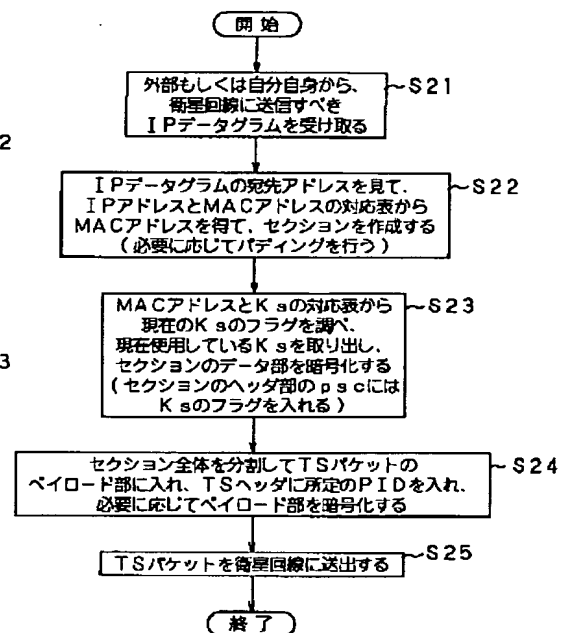
【図3】



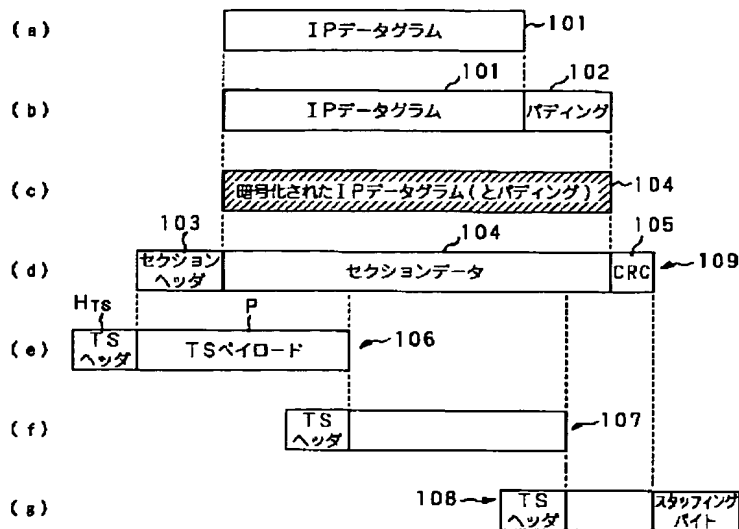
【図6】



【図10】



【図4】



【図8】

0	8	16	24	31
table_id	sa1	pl	revd	section_length
MAC_address_5	ravd	psc	asc	section_number
MAC_address_4	MAC_address_3	MAC_address_2	MAC_address_1	

sa1: section\_syntax\_indicator  
 pl: private\_indicator  
 revd: reserved  
 psc: payload\_acramble\_indicator  
 asc: address\_acramble\_indicator  
 LSf: LLC\_SNAP\_flag  
 enl: current\_next\_indicator

【図9】

MACアドレス	Ks_even	Ka_odd	Ksフラグ
08:00:46:01:07:24	0xC08F...25	0x90B3...AF	0
08:00:46:01:07:09	0x26D2...61	0xBA02...3C	1
01:00:5e:16:0:0	0x461E...67	0xDC1A...22	0

【図12】

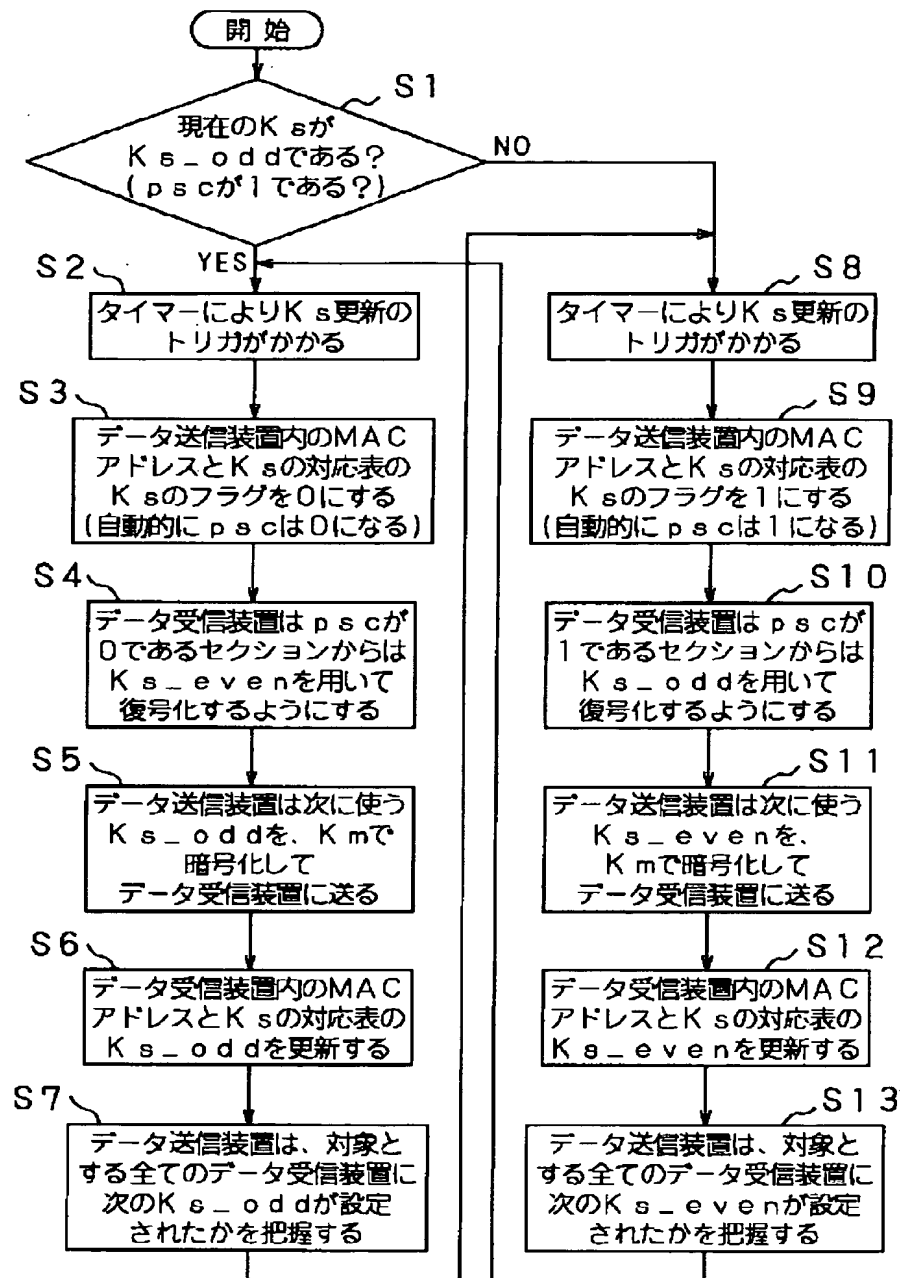
IPアドレス	bitmask	MAC address
133.11.9.39	255.255.255.225	08:00:46:01:07:24
133.11.20.0	255.255.255.0	08:00:46:01:07:09
226.0.0.0	255.255.255.224	01:00:5e:16:0:0

【図13】

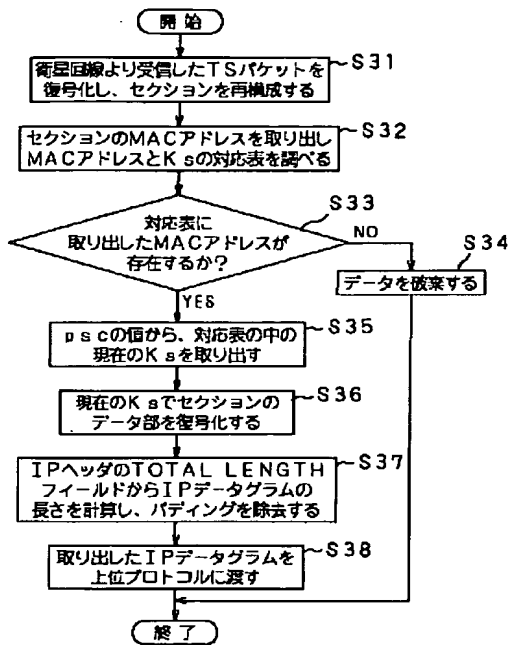
MACアドレス	Ks_even	Ka_odd
08:00:46:01:07:24	0xC08F...25	0x90B3...AF
01:00:5e:16:0:0	0x461E...67	0xDC1A...22



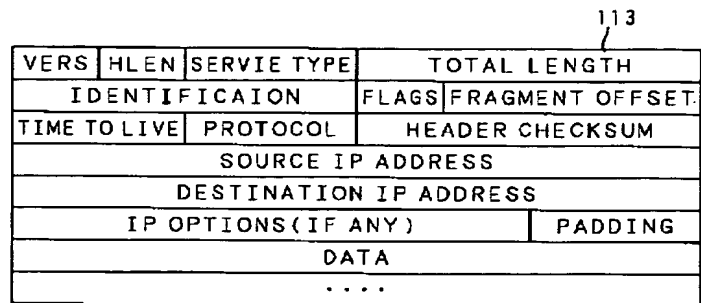
【図7】



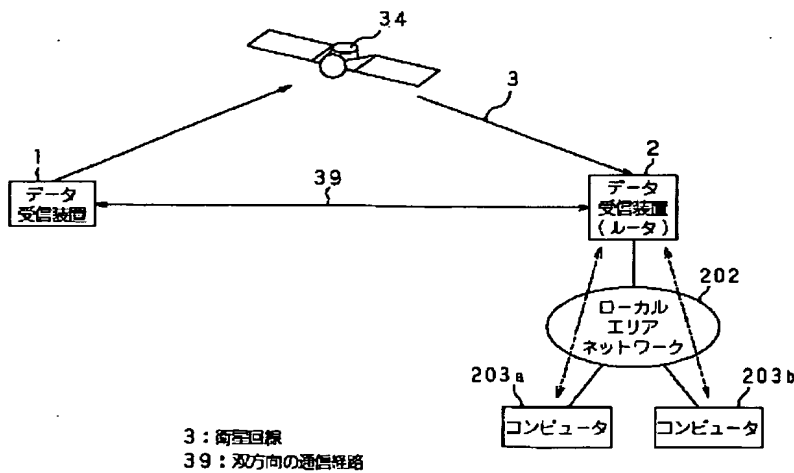
【図11】



【図14】



【図15】



【図16】

